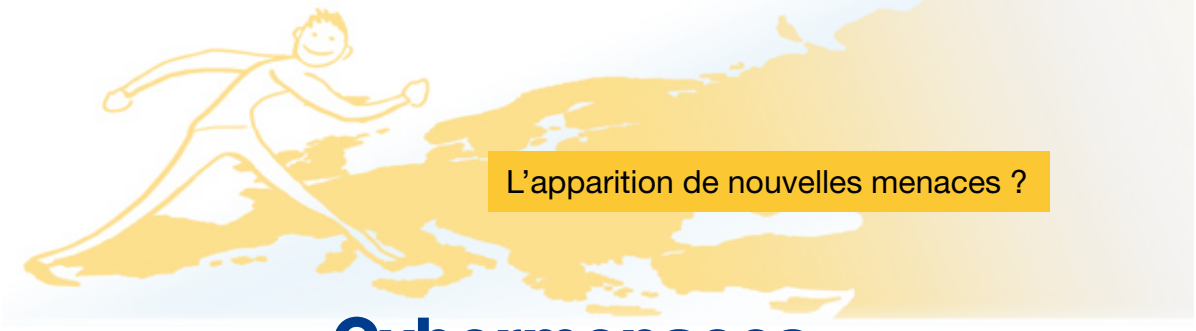

Cybermenaces, cyberguerres et cyberterrorisme en et contre l'Europe

Éric Filiol
Directeur de la recherche à l'ESIEA Ouest (Ecole supérieure d'informatique, électronique, automatique) - Directeur du Laboratoire de cryptologie et de virologie opérationnelles

Dès son avènement, le XXI^e^ siècle a été placé sous le signe du « cyber » et les termes de cyberguerre, cybercriminalité, cybermenaces ont envahi nos espaces médiatiques. L'attaque perpétrée contre l'Estonie – pays européen, membre de l'OTAN – en 2007, ainsi que, plus récemment, celles ayant visé des entités nationales ou économiques (attaque contre le ministère français des Finances en mars 2011, contre le FMI en juin 2011, contre le site de la CIA en juin 2011...) ont bouleversé notre vision du monde et montré combien la propagation de l'informatique et des réseaux est probablement devenue un facteur de faiblesse des États modernes. Il s'agit assurément d'une nouvelle dimension (Filiol, 2010) dans notre espace, avec laquelle il va falloir compter et vis-à-vis de laquelle les États travaillent à décliner, dans la dimension digitale, les contrôles et les protections jusque-là réservés au monde physique : cyberpolice, lutte informatique défense/offensive, filtrage de l'internet, intelligence numérique, cybercensure... De ce point de vue, la dimension « cyber » s'ajoute aux menaces dans un monde en perpétuelle évolution.

Un contexte nouveau

Toutefois cette dimension porte en elle des spécificités à nulle autre pareilles, lesquelles sont de nature non seulement à remettre en cause un certain nombre de concepts fondateurs mais également à donner naissance à de nouveaux (des)équilibres :

• L'oblitération du temps, de l'espace et de la notion de preuve (Filiol, 2010) a été intégrée dans la réflexion des décideurs. Un attaquant peut désormais frapper instantanément, à partir de n'importe quel point du globe et ce, sans laisser ni trace ni moyens de l'identifier et de le confondre ou, pire encore, en ouvrant la possibilité d'incriminer à tort des tiers innocents. Sur ce dernier point, le corollaire est la disparition des concepts de droit (national, international) et d'éthique.

• L'émergence tous azimuts d'une asymétrie croissante permettant à des acteurs de moindre importance (petits États, individus ou groupes d'individus) de remettre en cause le *leadership* d'acteurs majeurs (grands États, multinationales, organismes internationaux ou supranationaux) crée une situation géostratégique sans précédent. L'omniprésence de l'informatique et des réseaux ainsi que l'impossibilité de toute forme de contrôle sur les connaissances qui y sont liées permettent à des individus d'instaurer un rapport du faible au fort totalement différent. De ce point de vue, les États occidentaux, notamment d'Europe, du fait d'une dépendance totale vis-à-vis de la technologie et plus spécialement de la technologie de l'information, se trouvent beaucoup plus fragilisés que les États du Sud. La fracture numérique, dans le domaine de la sécurité des États, tourne à l'avantage de ceux qui en sont victimes sur le plan économique.

• Du fait de cette dépendance vis-à-vis de la technologie de l'information – laquelle gouverne désormais tous les autres secteurs, en particulier par l'informatisation, le contrôle à distance et les réseaux –, tout problème grave de sécurité affectant ces technologies fera avant tout des victimes civiles. La sophistication croissante des techniques de guerre (infanterie, marine, aviation, chimique, nucléaire, biologique puis, enfin, informatique) s'accompagne d'une augmentation proportionnelle du nombre de victimes civiles potentielles, engendrée par leur utilisation. De nos jours, la moindre des ressources (santé, fourniture d'eau, d'électricité, services bancaires, impôts, etc.) ayant un rôle important dans nos vies est gérée informatiquement.

• Le contrôle véritable de ces technologies (Filiol, 2011) échappe à la sphère étatique et régalienne et devient l'apanage des nouvelles générations – qui sont nées avec la dimension « cyber », voire ont directement contribué à sa naissance et à sa montée en puissance. Le développement du phénomène *hacker* est particulièrement significatif et accentue l'asymétrie précédemment évoquée. Avec lui, une nouvelle forme de contestation et de conscience collective/politique est en train de naître, au point de supplanter les frontières géographiques : nous assistons à l'émergence de ce qui pourrait bien être une véritable « internationale *hacker* », exerçant de fait LE véritable contrôle sur la sphère technologique au détriment des décideurs qui sont dépassés par cette révolution autant technologique que culturelle.

Le contexte sociétal a également évolué : la technologie informatique, sa fiabilité et la capacité des décideurs et responsables étatiques à assurer la sécurité de ces technologies suscitent de nombreuses peurs au sein des populations occidentales (SOFRES, 2010). Toute attaque informatique (ponctuelle et/ou généralisée) ayant pour résultat d'affecter gravement un ou plusieurs systèmes dont dépendent les citoyens peut avoir un impact dramatique sur la société. C'est précisément ce qu'a démontré, en 2007, l'attaque contre l'Estonie (Evrard, Filiol, 2007) qui a provoqué le blocage momentané de la vie économique de tout un pays (voir encadré).

La cyberattaque de 2007 contre l'Estonie

Les sites institutionnels estoniens ont été bloqués durant plusieurs jours en mai 2007 par des attaques en déni de service distribué (DDOS) d'une ampleur sans précédent à l'échelle d'un pays. La méthode utilisée a consisté à mettre hors service les serveurs web du pays, noyés sous un flot de demandes arrivant par milliers chaque seconde ; les requêtes émanaient d'une multitude de machines réparties dans le monde afin d'empêcher de leur bloquer l'accès par un simple filtrage. Ces attaques faisaient suite aux émeutes provoquées par la décision des autorités de déplacer un monument aux morts de l'Armée rouge, dédié aux soldats soviétiques qui ont « libéré » le pays en 1944. Les sites des banques et des sites gouvernementaux ainsi que la plupart des ressources critiques de l'Estonie – 90 % des services sont gérés par Internet ce qui fait de l'Estonie la plus grande e-démocratie - ont été paralysés durant plusieurs jours. La Russie a aussitôt été mise en accusation, mais sa responsabilité n'a jamais pu être prouvée.

On assiste donc à l'émergence de nouvelles formes de menaces liées au numérique, en premier lieu le « cyberterrorisme ». Il existe de multiples définitions du terme terrorisme, mais un certain consensus semble acquis concernant la perception générale de ce phénomène, comme le souligne Jacques Derrida (Derrida, 2004) : « La référence à un crime contre la vie humaine en violation des lois (nationales ou internationales) y impliquant à la fois la distinction entre civil et militaire (les victimes du terrorisme sont supposées être civiles) et une finalité politique (influencer ou changer la politique d'un pays en terrorisant sa population civile) ».

L'extension à la dimension « cyber » a, quant à elle, été plus simple, comme en témoigne la définition proposée par Kevin G. Koleman (Reis, 2008) : « Le cyber terrorisme peut aussi être défini beaucoup plus généralement, par exemple, comme 'L'utilisation préméditée des activités pertur-batrices, ou la menace de celle-ci, contre des ordinateurs et/ou réseaux, dans l'intention de causer un préjudice financier ou encore social, idéologique, religieux, politique ou autres objectifs. Ou pour intimider toute personne dans la poursuite de tels objectifs' ».

Il est désormais évident que les nouvelles menaces seront de type terroriste et auront pour principal ressort le détournement des technologies ayant un impact majeur sur les populations. En premier lieu, les cyberattaques passent par ou visent avant tout les technologies de l'information et des réseaux. L'ère des conflits militaires et autres confrontations violentes conventionnelles est donc peut-être en passe d'être révolue, pour laisser place à des menaces reposant sur une granularité plus fine des acteurs que des victimes mais également des moyens.

L'approche opérationnelle

L'analyse des doctrines rendues publiques et des attaques récentes, ainsi que des résultats de recherches dans ce domaine, permet de se faire une idée précise de l'approche opérationnelle des attaquants.

La Chine, premier pays à avoir formalisé les choses de manière à la fois rigoureuse et exhaustive, est devenue le modèle en la matière. L'extrait suivant résume à lui seul toute cette pensée opérationnelle : « Par exemple, alors que l'ennemi ne s'y attend pas du tout, l'assaillant mobilisera secrètement une masse de capitaux et lancera une attaque surprise contre ses marchés financiers ; après

avoir provoqué une crise financière, il opèrera une attaque de ses réseaux grâce à des virus implantés à l'avance dans les systèmes informatiques de l'adversaire et à l'intervention d'équipes de pirates informatiques. Il provoquera ainsi l'effondrement total du réseau électrique civil, du réseau de régulation des transports, du réseau de transactions boursières, des réseaux de télécommunications et des réseaux médiatiques, déclenchant une panique sociale, des troubles civils et une crise gouvernementale. Pour finir, une puissante armée massée aux frontières augmentera progressivement l'emploi des moyens militaires jusqu'à acculer l'ennemi à signer un traité sous la contrainte » (Qiao & Wang, 1999).

Le maitre mot est ici « l'effet domino » (Filiol & Raynal 2009, Filiol 2009, Filiol 2010) : l'analyse des systèmes critiques – le degré de criticité dépend lui-même de la cible et de l'effet final à obtenir –, de leurs interdépendances ainsi que de leurs dépendances vis-à-vis de composantes externes (humaines, techniques, organisationnelles...) permet de faire tomber un système en en frappant un autre, en apparence moins critique et par conséquent peu ou pas sécurisé, mais dont il dépend au regard d'une série de liens fonctionnels plus ou moins longue. La capacité opérationnelle ne repose donc plus tant sur la force de frappe elle-même que sur la capacité à identifier ces chaînes de dépendances. Le renseignement (information et connaissance préalable) est donc primordial.

Les *hackers* sont les bras armés de ces nouvelles formes de menaces : ils ont accès à l'ensemble des moyens et connaissances techniques (Filiol, 2011) ; ils sont au cœur de ces systèmes, à la création desquels ils ont souvent contribué. Mais ils n'étaient jusque-là que le bras armé d'une pensée opérationnelle précise (mafias, groupes terroristes classiques, États voyous, organismes gouvernementaux...).

L'avènement récent de groupes comme les *Anonymous* ou les *Lulzsec* (voir encadré) montre clairement une évolution significative vers l'émergence d'une conscience collective sinon politique, en tant que telle, dont le résultat serait la fusion des capacités opérationnelles et techniques. Ce cocktail assurément détonant est précisément de nature à remettre en cause tous les équilibres actuels.

Anonymous, *LulzSec*, émergence d'une conscience collective ?

Anonymous représente le concept de chacun et tous comme un collectif sans nom. Ce mouvement désigne un ensemble décentralisé constitué de plusieurs communautés formées d'internautes agissant de manière anonyme, dans un but particulier, *via* des actions coordonnées, informatiques et physiques. Certaines actions prennent la forme d'attaques par déni de service, lancées contre des sites ciblés comme ennemis des valeurs défendus par le mouvement. Lors des manifestations physiques du collectif, les membres sont généralement masqués. Ils défendent le droit à la liberté d'expression sur internet et en dehors. Ce mouvement a lancé récemment plusieurs attaques en Europe et aux Etats-Unis contre la scientologie, en faveur du fondateur de Wikileaks Julian Assange, mais a aussi soutenu les dissidence iranienne, tunisienne, égyptienne, malaise...

Apparu plus récemment, le groupe de *hackers LulzSec* revendique, lui, des attaques plus ludiques, essentiellement perpétrées contre des sites de jeux vidéo (Nintendo, Bethesda Softworks, SonyPictures.com...), mais également contre la CIA.

© AFP/ Javier Soriano, 2011

Les Goya, festival de cinéma espagnol, qui se sont déroulés à Madrid le 13 février 2011, ont été perturbés par une manifestation des *Anonymous*, qui protestaient contre la loi Sinde, qui lutte contre le piratage de la même façon que la loi Hadopi en France.

Le plan technique

Qu'une attaque soit unique ou fasse partie d'un scénario plus vaste et plus complexe, quelles en sont les « briques de base » ? La doctrine chinoise évoquée plus haut est explicite à ce sujet (Qiao & Wang, 1999) : « La première règle dans la guerre sans limite est qu'il n'y a aucune règle, rien n'est interdit [...]. Il n'existe rien au monde qui ne puisse devenir une arme ».

Dans un monde hypertechnologique, l'approche technique consiste à détourner des sciences et des techniques, en vue de produire un effet local de nature à déclencher l'effet domino évoqué précédemment. Du point de vue de l'attaquant, toutes les techniques et technologies sont par nature duales. Il suffit de les comprendre pour savoir comment les détourner à son profit et les combiner de manière redoutable. Le nombre des possibilités est alors infini ; celui de leurs combinaisons l'est encore plus. Ces attaques peuvent venir de n'importe où et, surtout, être le fait de n'importe qui ayant une bonne connaissance technique. La force des Anonymous réside avant tout dans la dispersion, la variété et le nombre de ses acteurs, et moins dans leur anonymat. La menace devient une hydre ayant des millions de têtes.

Contrairement au sentiment encore largement prévalent, ces attaques ne se contentent pas d'utiliser la seule dimension informatique. Certes, le plus souvent, le réseau internet est le vecteur idéal mais il est important de conserver à l'esprit que toute technologie (y compris les services qu'elle délivre) peut être utilisée et détournée. Ainsi, les attaques par nuages de micro- ou nanodrones[1] (Beaudoin & Gademer 2010, Avanthey *et alii*, 2011), les attaques des places boursières par détournement des outils utilisés en toute légalité par les *traders* eux-mêmes (Erra, 2011), le détournement des réseaux téléphoniques mobiles pour des communications intraçables (Desnos & Gueguen, 2001)... constituent des exemples particulièrement graves des nouvelles formes de terrorisme. L'attaque du 11 septembre 2001 – détournement d'avions transformés en missiles – n'a fait qu'annoncer cette tendance lourde. Une attaque coordonnée (Filiol, 2011) combinera toutes ces « briques de base », conventionnelles ou digitales.

Quelques réponses européennes

Face à ces menaces, l'Europe tente de s'organiser mais avec les difficultés propres à toute communauté d'États qui considèrent que ce domaine relève avant tout de leur sphère régalienne propre. En effet, ces menaces remettent potentiellement en cause la sécurité des États, lesquels n'entendent pas sous-traiter ou déléguer cette sécurité à une entité supra-nationale.

(1) Les microdrones sont des aéronefs sans pilote de moins de 500 g et d'une envergure inferieure à 50 cm. Les nano-drones ont un poids inférieur à 50 g et une envergure de moins de 15 cm. Des essaims de tels engins, communiquant entre eux pour une action coordonnée, peuvent transporter des charges explosives réduites, des substances chimiques ou biologiques. Leur coût réduit les rend accessibles au plus grand nombre.

Toutefois, depuis 2007, différentes initiatives ont vu le jour :

- Dans un cadre communautaire, annonce a été faite, en mai 2011, de la création d'équipes européennes de cyberdéfense, sur le modèle des Centres nationaux d'intervention (CERT – *Computer Emergency Response Team*), regroupées sous une entité unique dès 2012/2013[2] ;
- De son côté l'OTAN a créé, depuis 2008, un Centre de recherche et de formation de l'OTAN consacré à la cyberdéfense (CCDCOE - *NATO Cooperative Cyber Defence Centre of Excellence*)[3]. Situé à Tallinn (Estonie), il bénéficie pour le moment de la contribution d'un nombre limité de pays (Allemagne, Espagne, Estonie, Italie, Lettonie, Lituanie, Roumanie et Slovaquie) ;
- En novembre 2010 a été annoncée la mise en œuvre d'une collaboration tripartite OTAN, Union européenne et États-Unis[4].

Il est trop tôt encore pour déterminer si ces initiatives auront une réelle efficacité et ne se résument pas à des déclarations d'intentions qui, finalement, ne résisteront pas aux volontés nationales de conserver jalousement leur prérogatives. Si les Etats-Unis ont une vision plus claire de la situation (mais aussi plus manichéenne et plus simpliste) et, de fait, peuvent se targuer d'une certaine avance, l'Union européenne a cependant des atouts de taille qui, à terme, sont susceptibles de lui permettre de mieux se protéger. Elle possède, notamment, une capacité et une volonté de régulation qui lui permettent, contrairement aux États-Unis, d'imposer ses vues sur la sphère privée *via* l'approche législative. En Europe, le bien commun prévaut sur la sphère économique privée ; il est donc possible d'agir en amont sur les acteurs industriels impliqués. Si l'Union européenne est, à ce jour, moins dépendante des réseaux et de l'informatisation des systèmes critiques ou, du moins, impose des règles drastiques, privilégiant encore la sécurité sur les services, on peut toutefois se demander pour combien de temps encore, notamment face à la pression des marchés ?

L'évolution vers des sociétés hypertechnologiques a longtemps été considérée comme un but idéal pour le plus grand bonheur des populations, au point d'en faire l'indicateur quasi unique du degré de civilisation. Mais la forte dépendance qui en résulte se traduit par une vulnérabilité et une fragilisation de nos sociétés sans équivalent dans l'histoire de l'humanité. Un nombre réduit d'individus peut désormais, en détournant à son profit les ressources technologiques existantes, bouleverser les équilibres actuels. Contrairement aux

(2) **http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf**.
(3) **http://www.ccdcoe.org/**.
(4) **http://www.5min.com/Video/EU-US-and-NATO-to-Work-Together-on-Cyber-Defense-510471543**.

menaces antérieures, il n'existe aucun contrôle et aucune traçabilité ni des acteurs ni des outils (armes) possibles. Ils sont partout parmi nous, au cœur même de nos sociétés.

Bibliographie

- L. Avanthey, L. Beaudoin, A. Gademer et V. Germain (2011), « Potential Threats of UAV Swarms and the Countermeasure's Need », *10th European Conference on Information Warfare and Security*, ECIW 2011, Tallinn, Estonia.

- Laurent Beaudoin et Antoine Gademer (2010), « Towards symmetrization of asymmetric air dominance : the potential key role playing by home-made low-cost Unmanned Aerial Systems », *9th European Conference on Information Warfare and Security*, ECIW 2010, Thessalonique, Greece.

- Jacques Derrida (2004), « Qu'est-ce que le terrorisme ? », *Le Monde Diplomatique*, **http://www.monde-diplomatique.fr/2004/02/DERRIDA/11005**

- A. Desnos et G. Gueguen (2001), « A "Mobile and Quick" Terrorism », *10th European Conference on Information Warfare and Security*, ECIW 2011, Tallinn, Estonia.

- Robert Erra (2011), « Malicious Flash Crack Attack by Quote Stuffing (This is the Way the Financial World Could End) », *10th European Conference on Information Warfare and Security*, ECIW 2011, Tallinn, Estonia.

- Philippe Evrard et Eric Filiol (2007), « Guerre, guérilla et terrorisme informatique : fiction ou réalité ». *Journal de la sécurité informatique MISC 33*, pp. 09-17, septembre-octobre.

- Philippe Evrard et Eric Filiol (2008), « Lutte informatique offensive : les 'bons', la 'brute' et les 'méchants' », *Journal de la sécurité informatique MISC 36*, pp. 22-31, mars.

- Philippe Evrard et Eric Filiol (2008), « Guerre, guérilla et terrorisme informatique : du trafic d'armes numériques à la protection des infrastructures », *Journal de la sécurité informatique MISC 35*, pp. 4-13, janvier.

- Eric Filiol (2009), « Operational Aspects of Cyberwarfare or Cyber-Terrorist Attacks : What a Truly Devastating Attack Could do », *Proceedings of the 8th European Conference on Information Warfare and Security 2009*, Lisbon, Portugal, pp. 71-79, 6-7 juillet.

- Éric Filiol et F. Raynal (2009), « Cyberguerre : de l'attaque du bunker à l'attaque dans la profondeur », *Revue de Défense nationale et sécurité collective*, volume 3, pp. 74-86, mars.

- Éric Filiol (2010), « *Aspects opérationnels d'une cyber attaque: renseignement, planification et conduite* », *in* D. Ventre (dir.), *Cyber guerre et guerre de l'information - Stratégies, règles et enjeux*, Ed. Hermès - Lavoisier, Paris.

- Éric Filiol (2011) « Paroles de hacker ». *Blog des Echos*, http://blogs.lesechos.fr/intelligence-economique/paroles-de-hacker-a5543.html, 11 avril.

- Col. Qiao, L. et Wang X. (1999), « Unrestricted Warfare », *People's Liberation Army*, Literature and Arts Publishing House, Beijing, Des extraits sont librement disponibles sur **http://www.cryptome.org/cuw.htm**

- Ricardo A. Reis (2008), « Cyberterrorism – A Case Study for Emergency Management », *International Consortium for Organization Resilience* (ICOR), **http://www.slideshare.net/ricardo.areis/cyberterrorism-presentation**

- Sondage SOFRES (2010), « Les préoccupations des Français », **http://www.sondages-en-france.fr/sondages/Actualit%C3%A9/Pr%C3%A9occupations#poll431**